

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-334

Vulnerability Summary for the Week of November 23, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
autodesk -- autodesk_softimage autodesk -- autodesk_softimage_xsi	Autodesk Softimage 7.x and Softimage XSI 6.x allow remote attackers to execute arbitrary JavaScript code via a scene package containing a Scene Table of Contents (aka .scntoc) file with a Script_Content element, as demonstrated by code that loads the WScript.Shell ActiveX control.	2009-11-24	9.3	CVE-2009-3576 BID BUGTRAQ MISC SECTRACK
autodesk -- 3ds_max	Autodesk 3D Studio Max (3DSMax) 6 through 9 and 2008 through 2010 allows remote attackers to execute arbitrary code via a .max file with a MAXScript statement that calls the DOSCommand method, related to "application callbacks."	2009-11-24	9.3	CVE-2009-3577 BID BUGTRAQ MISC SECTRACK
avast -- avast_antivirus_home avast -- avast_antivirus_professional	Heap-based buffer overflow in aswRdr.sys (aka the TDI RDR driver) in avast! Home and Professional 4.8.1356.0 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via crafted arguments to IOCTL 0x80002024.	2009-11-23	7.2	CVE-2009-4049 MISC VUPEN BID BUGTRAQ MISC SECUNIA
betsy -- betsy_cms	Directory traversal vulnerability in admin/popup.php in Betsy CMS 3.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the popup	2009-11-23	7.5	CVE-2009-4056 VUPEN MTS

	parameter.			MISC SECUNIA
cubecart -- cubecart	SQL injection vulnerability in includes/content/viewProd.inc.php in CubeCart before 4.3.7 remote attackers to execute arbitrary SQL commands via the productId parameter.	2009-11-23	7.5	CVE-2009-4060 XF VUPEN BID SECUNIA OSVDB CONFIRM
gforge -- gforge	SQL injection vulnerability in GForge 4.5.14, 4.7.3, and possibly other versions allows remote attackers to execute arbitrary SQL commands via unknown vectors.	2009-11-24	7.5	CVE-2009-4070 DEBIAN SECUNIA
hp -- operations_manager	HP Operations Manager 8.10 on Windows contains a "hidden account" in the XML file that specifies Tomcat users, which allows remote attackers to conduct unrestricted file upload attacks, and thereby execute arbitrary code, by using the org.apache.catalina.manager.HTMLManagerServlet class to make requests to manager/html/upload.	2009-11-23	10.0	CVE-2009-3843 XF MISC OSVDB SECTRACK SECUNIA HP HP
inertialfate -- com_if_nexus	SQL injection vulnerability in the inertialFATE iF Portfolio Nexus (com_if_nexus) component 1.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in an item action to index.php.	2009-11-23	7.5	CVE-2009-4057 XF BID MISC SECUNIA OSVDB
opera -- opera_browser	Unspecified vulnerability in Opera before 10.10 has unknown impact and attack vectors, related to a "moderately severe issue."	2009-11-24	10.0	CVE-2009-4072 BID CONFIRM CONFIRM CONFIRM
php -- php	** DISPUTED ** mainstreams/plain_wrapper.c in PHP 5.3.x before 5.3.1 does not recognize the safe_mode_include_dir directive, which allows context-dependent attackers to have an unknown impact by triggering the failure of PHP scripts that perform include or require operations, as demonstrated by a script that attempts to perform a require_once on a file in a standard library directory. NOTE: a reliable third party reports that this is not a vulnerability, because it results in a more restrictive security policy.	2009-11-23	7.5	CVE-2009-3559 CONFIRM CONFIRM MLIST MLIST MLIST
symantec -- altiris_deployment_solution symantec -- altiris_management_platform symantec -- altiris_notification_server	Buffer overflow in the RunCmd method in the Altiris eXpress NS Console Utilities ActiveX control in AeXNSConsoleUtilities.dll in the web console in Symantec Altiris Deployment Solution 6.9.x, Altiris Notification Server 6.0.x, and Management Platform 7.0.x allows remote attackers to execute arbitrary code via a long string in the second argument.	2009-11-25	9.3	CVE-2009-3033 CONFIRM
telebidauctionsclient -- telebid_auction_script	SQL injection vulnerability in allauctions.php in Telebid Auction Script allows remote attackers to execute arbitrary SQL commands via the aid parameter.	2009-11-23	7.5	CVE-2009-4058 XF MISC SECUNIA

Medium Vulnerabilities				
Back to top				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
joomclan -- com_joomclip	SQL injection vulnerability in the JoomClip (com_joomclip) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the cat parameter in a thumbs action to index.php.	2009-11-23	6.8	CVE-2009-4059 XF BID SECUNIA MISC OSVDB
anon-design -- printfriendly	Multiple cross-site scripting (XSS) vulnerabilities in the Printfriendly module 6.x before 6.x-1.6 for Drupal allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-23	4.3	CVE-2009-4062 BID CONFIRM CONFIRM
autodesk -- alias_wavefront_maya autodesk -- autodesk_maya	Autodesk Maya 8.0, 8.5, 2008, 2009, and 2010 and Alias Wavefront Maya 6.5 and 7.0 allow remote attackers to execute arbitrary code via a (1) .ma or (2) .mb file that uses the Maya Embedded Language (MEL) python command or unspecified other MEL commands, related to "Script Nodes."	2009-11-24	6.8	CVE-2009-3578 BID BUGTRAQ MISC SECTRACK
dovecot -- dovecot	Dovecot 1.2.x before 1.2.8 sets 0777 permissions during creation of certain directories at installation time, which allows local users to access arbitrary user accounts by replacing the auth socket, related to the parent directories of the base_dir directory, and possibly the base_dir directory itself.	2009-11-24	4.6	CVE-2009-3897 MLIST MLIST MLIST
drupal -- drupal paul_beaney -- phplist	Multiple cross-site request forgery (CSRF) vulnerabilities in the "My Account" feature in PHPLIST Integration module 5 before 5.x-1.2 and 6 before 6.x-1.1 for Drupal allow remote attackers to hijack the authentication of arbitrary users via vectors related to (1) subscribing or (2) unsubscribing to mailing lists.	2009-11-23	6.8	CVE-2009-4066 BID CONFIRM CONFIRM CONFIRM
ezra_barnett_gildesgame -- og_subgroups	Cross-site scripting (XSS) vulnerability in the Subgroups for Organic Groups (OG) module 5.x before 5.x-4.0 and 5.x before 5.x-3.4 for Drupal allows remote attackers to inject arbitrary web script or HTML via unspecified node titles.	2009-11-23	4.3	CVE-2009-4063 BID CONFIRM CONFIRM
gforge -- gforge	Cross-site scripting (XSS) vulnerability in www/help/tracker.php in GForge 4.5.14, 4.7 rc2, and 4.8.1 allows remote attackers to inject arbitrary web script or HTML via the helpname parameter.	2009-11-24	4.3	CVE-2009-3303 BID DEBIAN CONFIRM
gforge -- gforge	Multiple cross-site scripting (XSS) vulnerabilities in GForge 4.5.14, 4.7.3, and possibly other versions allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-24	4.3	CVE-2009-4069 DEBIAN
igor_sysoev -- nginx nginx -- nginx	src/http/ngx_http_parse.c in nginx (aka Engine X) 0.1.0 through 0.4.14, 0.5.x before 0.5.38, 0.6.x before 0.6.39, 0.7.x before 0.7.62, and 0.8.x before 0.8.14 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a long URI.	2009-11-24	5.0	CVE-2009-3896 CONFIRM MLIST MLIST

igor_sysoev -- nginx nginx -- nginx	Directory traversal vulnerability in src/http/modules/ngx_http_dav_module.c in nginx (aka Engine X) before 0.7.63, and 0.8.x before 0.8.17, allows remote authenticated users to create or overwrite arbitrary files via a .. (dot dot) in the Destination HTTP header for the WebDAV (1) COPY or (2) MOVE method.	2009-11-24	4.9	CVE-2009-3898 MLIST MLIST MLIST MLIST MLIST
isc -- bind	Unspecified vulnerability in ISC BIND 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, 9.7 beta before 9.7.0b3, and 9.0.x through 9.3.x with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks via additional sections in a response sent for resolution of a recursive client query, which is not properly handled when the response is processed "at the same time as requesting DNSSEC records (DO)."	2009-11-25	5.8	CVE-2009-4022 CONFIRM
jeff_miccolis -- strongarm_module	Cross-site scripting (XSS) vulnerability in the settings page in the Strongarm module 6.x before 6.x-1.1 for Drupal allows remote attackers to inject arbitrary web script or HTML via the value field when viewing overridden variables.	2009-11-23	4.3	CVE-2009-4065 BID CONFIRM CONFIRM
linux -- kernel	The fuse_direct_io function in fs/fuse/file.c in the fuse subsystem in the Linux kernel before 2.6.32-rc7 might allow attackers to cause a denial of service (invalid pointer dereference and OOPS) via vectors possibly related to a memory-consumption attack.	2009-11-25	4.9	CVE-2009-4021 CONFIRM XF BID MLIST MLIST CONFIRM CONFIRM
microsoft -- ie	The printing functionality in Microsoft Internet Explorer 8 allows remote attackers to discover a local pathname, and possibly a local username, by reading the dc:title element of a PDF document that was generated from a local web page.	2009-11-24	5.0	CVE-2009-4073 MISC BUGTRAQ MISC
microsoft -- ie	The XSS Filter in Microsoft Internet Explorer 8 allows remote attackers to leverage the "response-changing mechanism" to conduct cross-site scripting (XSS) attacks against web sites that have no inherent XSS vulnerabilities, related to the details of output encoding.	2009-11-25	4.3	CVE-2009-4074 MISC MISC MISC
mozilla -- bugzilla	Template.pm in Bugzilla 3.3.2 through 3.4.3 and 3.5 through 3.5.1 allows remote attackers to discover the alias of a private bug by reading the (1) Depends On or (2) Blocks field of a related bug.	2009-11-20	5.0	CVE-2009-3386 CONFIRM VUPEN BID CONFIRM
php -- php	PHP 5.2.11, and 5.3.x before 5.3.1, does not restrict the number of temporary files created when handling a multipart/form-data POST request, which allows remote attackers to cause a denial of service (resource exhaustion), and makes it easier for remote attackers to exploit local file inclusion vulnerabilities, via multiple requests, related to lack of support for the max_file_uploads directive.	2009-11-23	5.0	CVE-2009-4017 CONFIRM CONFIRM MLIST
puntolatinoclub -- gallery_assist_module	Cross-site scripting (XSS) vulnerability in the Gallery Assist module 6.x before 6.x-1.7 for Drupal allows remote attackers to inject arbitrary web script or HTML via node titles.	2009-11-23	4.3	CVE-2009-4064 BID CONFIRM CONFIRM

redmine -- redmine	Multiple cross-site scripting (XSS) vulnerabilities in Redmine 0.8.5 and earlier allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-25	4.3	CVE-2009-4078 XF VUPEN BID CONFIRM SECUNIA CONFIRM JVNDDB JVN JVN
roundcube -- roundcube_webmail	Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail 0.2.2 and earlier allows remote attackers to hijack the authentication of unspecified users for requests that modify user information via unspecified vectors, a different vulnerability than CVE-2009-4077.	2009-11-25	4.3	CVE-2009-4076 OSVDB MISC SECUNIA JVNDDB JVN
roundcube -- roundcube_webmail	Cross-site request forgery (CSRF) vulnerability in Roundcube Webmail 0.2.2 and earlier allows remote attackers to hijack the authentication of unspecified users for requests that send arbitrary emails via unspecified vectors, a different vulnerability than CVE-2009-4076.	2009-11-25	4.3	CVE-2009-4077 OSVDB MISC SECUNIA JVNDDB JVN
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the timeout mechanism in sshd in Sun Solaris 10, and OpenSolaris snv_99 through snv_123, allows remote attackers to cause a denial of service (daemon outage) via unknown vectors that trigger a "dangling sshd authentication thread."	2009-11-25	5.0	CVE-2009-4075 SUNALERT CONFIRM
yuriy_babenko -- agreement_module	Multiple cross-site scripting (XSS) vulnerabilities in the Agreement module 6.x before 6.x-1.2 for Drupal allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-11-23	4.3	CVE-2009-4061 BID CONFIRM CONFIRM

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
opera -- opera_browser	Opera before 10.10, when exception stacktraces are enabled, places scripting error messages from a web site into variables that can be read by a different web site, which allows remote attackers to obtain sensitive information or conduct cross-site scripting (XSS) attacks via unspecified vectors.	2009-11-24	3.5	CVE-2009-4071 CONFIRM CONFIRM CONFIRM
redmine -- redmine	Cross-site request forgery (CSRF) vulnerability in Redmine 0.8.5 and earlier allows remote attackers to hijack the authentication of users for requests that delete a ticket via unspecified vectors.	2009-11-25	3.5	CVE-2009-4079 XF VUPEN BID MISC SECUNIA MISC JVNDDB JVN

[Back to top](#)

Last updated November 30, 2009

 [Print This Document](#)